Solutionary™
reliable, responsible e-security

0 1 1 0 HOW TO PROTECT INFORMATION: 1 1 1 0 1 0 0 1 0 1 0 1 0 1 0 0

A COMPREHENSIVE GUIDE TO SECURING NETWORKS AND SYSTEMS

www.solutionary.com • 866.333.2133

Introduction

Promising a "Comprehensive Guide to Securing Networks and Systems," may connote an attempt to provide a checklist for securing all of the systems and applications found in today's complex computing world. That is not the focus of this paper, nor is it one that could be covered in anything less than several hundred pages of documents.

Rather, this document attempts to provide a roadmap for the creation of a secure infrastructure, which is the basis for comprehensively addressing the security needs of any size organization. It offers step-by-step information on processes and procedures needed to provide a more secure network environment, both for corporate networks and home users. It also provides tips, advice and words of warning on applying these tools to your situation.

Learning everything you need to know about information security may take more time and more study. But, as with most things, the best place to start is with the basics – what we call the Six Steps to Better Security. The more masterfully you apply these principles, the more comprehensive your information security will be, both now and into the future.

Time and Place in History

Security practices were not always commonplace at the home or the office. Perhaps you remember a time when many people could leave their doors unlocked at night and their keys in their car without fear. In fact, many businesses used to rely on the honor system to receive payment for goods and services rendered. Times have changed in the world of physical security, and the desire to protect assets, as well as life and health, has led nearly everyone to step-up the level of security in their daily lives. Locking doors at night is now standard practice for most of us. Security systems in homes and cars have become commonplace, a preoccupation that has led to an increasing acceptance of the inconveniences security systems cause in the workplace.

However the need and function of security has not similarly evolved in the IT world. The attitude towards electronic crime has been much slower to develop than the acceptance of physical security. How many employees would consider breaking into the HR department's filing cabinets to locate private salary information? Yet, those very same people may not see a problem with retrieving the same information from a database with weak access control. Similarly, a person who wouldn't dream of breaking and entering may portscan a computer with reckless abandon.

That is where we find a major disconnect. When CNN or ABC runs a story on hacking, it invariably deals with well-known targets, because Microsoft, the White House and E-Trade all make good headlines. But every day throughout the world, servers, PC's, and networks are probed for vulnerabilities, and a staggering number of them are exploited, often times without the knowledge of their owners. The key to curbing this devastating trend is improved security.

Six Steps to Better Security

Step 1: Organize a security steering committee

Any comprehensive security plan needs widespread support if there is to be any hope of success. One of the best methods for gaining support is the establishment of an enterprise-wide security committee. This committee should be made up of representatives from each department as well as corporate officers who might improve the chances that the security plan will be accepted, not just by the users but by the corporation as a whole.

This security steering committee serves many purposes. First, it ensures that users' concerns will be voiced during the creation of the plan, instead of during deployment when it's often too late to make changes. The committee also provides a communication vehicle for all aspects of information security. Through the initial assessment and information gathering, the committee can garner and provide feedback on the asset and information valuations, as well as determine the level of acceptable risk.

The steering committee should also look for efficiency gains and cost savings that can come about as part of the security process. For example, installing security systems and procedures across the enterprise is more effective, from both a security and cost standpoint, than having each department create their own. Also, being proactive rather than reactive to security incidents saves money, time and stress.

Finally, an enterprise-wide security committee can change business practices when necessary to increase security while also improving productivity, quality and efficiency and make these new practices a part of the company culture. Examples of this are implementing a VPN (Virtual Private Network) to allow employees to securely check e-mail and work on documents from home, or splitting a job function between two employees or departments.

A final note: The security steering committee should not end after the initial security rollout, but should remain as the communication vehicle for future security enforcement discussions, issues, and improvements. As the business needs and climate change, so does risk. Keeping the security committee involved in current and future business directions ensures risks are adequately managed.

Step 2: Gather information

Before embarking on any type of security implementation, you must conduct a comprehensive audit, including not only the devices and systems involved in the security implementation, but also the business processes, security awareness, and assets and information protected. It is important to note that the audit provides only a point-in-time snapshot of the current status of enterprise security. This audit also must include a comprehensive review of a corporation's security policies and procedures, as well as any disaster recovery or business continuance plans in place.

To determine the level of vulnerability, begin at the highest-risk entry point to your network(s): the Internet. A full External Assessment conducted by a reputable firm can provide the information necessary to evaluate the current level of security protecting your network from Internet-based attack. A full External Assessment will include not only a standard penetration and vulnerability test, but also the analysis of home-users, VPN-connected systems and networks, the analysis of publicly available information, as well as ACD and voicemail penetration, and can often include social-engineering attacks. This is much of the same information that is gathered and shared among hackers on a daily basis, and not knowing how you appear to the rest of the world makes it difficult, if not impossible, to determine how vulnerable you are.

One of the most important considerations in an External Assessment is the point from which the assessment is conducted. Typically, a company will conduct an Assessment from the Internet, providing an external view of their e-mail and web servers. Companies are starting to recognize that not all attacks come from the Internet. Providing a security layer around their accounting and HR system, protecting themselves from VPN users and partners, and separating corporate networks from public access terminals are all areas that can benefit from an External Assessment. As the old adage goes, "Good fences make good neighbors."

An Internal Assessment also can provide a great deal of insight into the current state of security in your organization. By thoroughly examining your business and security policies and processes, and validating that data against what is implemented, compliance with existing standards can be assessed. An Internal Assessment can also provide the same detail of information as an External Assessment, although with the firewall removed, the servers and systems can be probed to a much deeper extent, even to include running password cracking and system analysis tools to further verify policy compliance.

Step 3: Assess the risk

When assessing risk, consider the following formula:

Risk = Asset Value * Vulnerability * Likelihood of exploit

Risk is equal to the value of the asset in question (including dollar value, cost of downtime, as well as intangibles like loss of customer trust), times the extent of vulnerability (total/partial loss of data, system downtime, damage or corruption of data), times the likelihood of the exploit occurring.

Take the results from the first step (the assets, the External Assessment report and the security policy), and look at the three from a common vantage point. Then, start to ask some tough questions.

- Does your existing security policy properly address and provide sufficient protection?
- Do the results from the External Assessment validate the policy?
- Are weaknesses identified in the Assessment that aren’t addressed in the policy?
- Does the level of security coincide with the level of risk?
- What assets/information incur the highest risk?

The answers to these questions provide a starting point for a comprehensive analysis of the thoroughness of your policy. Perhaps the most important information gathered from this step is the combination of the value of the asset and the corresponding risk. By evaluating this information, you can look for solutions that address the global requirements, rather than getting micro-focused on individual problems. At the same time, you can generate a ‘hit list’ of the areas requiring the most immediate attention.

Step 4: Create the solution

Finding a 'plug-and-play' security solution is impossible in today's world-- especially when constrained by existing business rules and the need for compatibility with all of the applications, data flows and systems in place today. There is no silver bullet that can address all of the issues facing today's IT staff, nor a single vendor that can provide the necessary tools. By combining multiple vendors and products to create a comprehensive multi-layer security implementation, a company has the best chance of providing the level of security commensurate with the risk/value, while still allowing the business to function at a level necessary to ensure profitability. With all of that said, there are a few key areas all organizations need to address when searching for an effective plan.

Firewall

The firewall should be the starting point for any security tool/technology evaluation. This single piece of hardware/software is responsible for blocking more direct attacks on valuable information than any other. However, choosing a firewall is not as easy as it once was. Questions about feature sets, plug-in support, appliance versus server-based, and application or packet-filtering firewalls cloud the issues more than ever. Coupled with that is the need of many organizations to deploy a multi-layer firewall implementation that will properly address their security needs. This creates a wide assortment of possible technologies, vendors, products, and implementation possibilities. All firewalls are not created equal, and even within an individual organization there may be requirements for different types of firewalls-- depending upon the particular application, network configuration and environment. Sifting through this potpourri of information and propaganda to find the products that satisfy the business goals and security policies is the only task that matters. Our best advice is to ignore the fluff and focus on the basics.

Network Intrusion Detection System (IDS)

A firewall is only as good as what it blocks and as weak as what it lets pass. That is where an IDS comes into play. If you think of a firewall as a dam blocking a river, then consider the IDS as the system monitoring the flow of water on the other side. An IDS, by not becoming actively involved in the forwarding of packets, spends its cycles analyzing the packets the firewall allows through, looking for signatures of known attacks a firewall can't detect or successfully block. It is the first line of defense behind the firewall, and provides the necessary auditing and information to ensure the firewall is configured and working properly.

Host-based Intrusion Detection System (H-IDS)

The selection, implementation, and usage of a host-based intrusion detection system is more dependant upon the specific OS and application environment than any other section. A fully functioning H-IDS can provide timely notification of any changes made to a server whether intentional or unintentional. It is one of the best ways to minimize the damage from a server compromise, but it must be viewed as a reactionary measure. Finding a system that supports most or all of the OS's in use at your organization should be viewed as one of the primary decision points for an H-IDS.

Application-based Intrusion Detection System (App-IDS)

A growing number of application-based IDS's appearing on the market. These tools operate by either analyzing the event messages from a particular application, or by proxying the information to that application. While they are very specialized, they can provide increased security for their specific target application. And, when combined with a host-based IDS, they ensure that the impact from a compromised server is minimized. An App-IDS should be viewed as a purely supplementary security function, albeit an effective one under the proper circumstances.

Anti-Virus Software

One common mistake made with AV software has to do with its best location for deployment. To be truly effective, AV software should be on all workstations, servers, PDA's, systems, and most importantly, anywhere data flows to or from the Internet. The two most important things to consider when picking an AV vendor are management of multiple servers and workstations on a corporate scale and the vendor's ability to respond to new virus threats. (One caution: Never assume the software is working properly. Always check the version of the local virus database and ensure the engine is running.)

Virtual Private Network (VPN)

Using a VPN to provide employee or partner access to company resources from home or the road can provide a great level of security, cost-effective communication, and an overall increase in employee productivity. This does not come without risk, however. Anytime a VPN is implemented, you are extending the reach of your corporate, unprotected network to all nodes connected to the VPN termination point. To put this another way, the same PC an employee uses to play games and browse newsgroups is now a trusted part of a corporate network, creating what is often times a back-door, or the 'weakest-link' to a corporate network resource. To ensure the security of this system, the home user's systems must adhere to the same security policies and procedures as a corporate system. This can be accomplished through the use of a VPN vendor supporting client security profiles. By restricting the applications that can run on a home machine, the network ports that can be open, disabling split-tunneling, and forcing an updated anti virus engine to be running on the remote system, this risk can be minimized. This is especially important as companies face the constant threat of litigation, should their networks or systems be used to attack another company.

Two-Factor Authentication

Passwords provide little security. Worse, increasing password security by making users frequently change passwords often has a reverse effect: It forces them to write down their passwords. Augmenting or replacing passwords with any of the multi-factor security tokens and/or authentication systems on the market can greatly augment user-level security. The issues to consider when choosing a two-factor security system are application and operating-system support and system/device management overhead.

Biometrics

While biometrics have advanced greatly over the past several years, they still present many difficulties for a wide-reaching deployment as an e-security measure. Fingerprint, retina, voice, iris and hand-geometry sensors all provide security above passwords or two-factor alone, but as of today they are best implemented as barriers to physical access as opposed to system-level access. Many of these technologies also are difficult, if not impossible, to deploy in many industries and environments (i.e. using fingerprint scanners in environments where employees must wear gloves). Still, technological and management advances over the next several years will create the necessary affordability, scalability and functionality to make biometrics a viable option for desktop authentication.

Smart cards

Smart cards have come a long way over the past couple years in terms of support, manageability and implementation. A recent push by credit-card companies has resulted in heightened levels of awareness of this technology, as well as an increase in its affordability. Windows 2000 provides native support for smart cards as a primary means of login authentication, making it truly viable for enterprise-wide rollout in some organizations. Additionally, the combination of multiple technologies (i.e. proximity, mag-stripe, and smart card) in a single card finally presents organizations with a comprehensive approach to both logical and physical access control.

Server Auditing

A constant practice of auditing the level of security provided by servers is essential to proper security management. This auditing should, as previously discussed, begin from the Internet. Any time a new exploit is published or vulnerability discovered, every server in an enterprise should be audited from the Internet to determine if it is exposed. Additionally, internal auditing and assessment of servers on a scheduled basis is necessary to minimize the security risk, should a firewall fail or another server or system be compromised.

Most operating systems come out of the box set to a minimal level of security with many known vulnerabilities. Before a server is placed in production, a process of 'hardening' should be applied. All of the latest patches and bug fixes should be installed on the server, and any unnecessary services should be disabled. This can greatly reduce the risk on these machines.

Continually monitoring audit and event logs from servers and applications provides some of the best information about, and insight to, security attacks. In many cases, it is the only way to determine the true extent of an attack and should be viewed as the most important part of incident analysis.

Application Auditing

The source of nearly every security issue is poor application programming. This is not limited to off-the-shelf products, but applies to any application, whether purchased, freely downloaded or internally-developed. To help minimize the risk of application security issues, constantly assess the applications in use by your corporation, as well as the standards and practices used by internally-developed applications. This should include any applications to which external entities, like partners or customers, can access.

Monitoring the security configuration of applications can often increase the level of security. Most applications come configured at a minimal level of security, but through configuration tools this security level can often be increased. The amount of audit information provided by applications is often configurable, as well. Where applications do provide security event information, the timely auditing and analysis of this information is key to detecting security-related issues.

Operating Systems

The selection of an operating system and application is a very tricky process in most organizations. The 'Microsoft vs. UNIX' battle is, in many cases, likened to a religious fervor, and has deep-seeded feelings on all sides. When choosing an O/S, the particular vendor is not nearly as important as the vendor's ability to repair security issues in a timely manner and the ease with which the repairs can be implemented. Any operating system from two years ago is insecure by today's standards, and keeping your servers and applications updated will help minimize the risks presented, regardless of the vendor. When selecting an operating system, consider not only the normal criteria (manageability, performance, reliability), but also the applicability of that O/S to your particular application. One O/S may provide security better suited to a DNS or web server, while others may function better as an application, database or e-mail server.

Enterprise Event Correlation

Many possible security events are constantly logged by firewalls, IDS's, servers and applications. Selecting a system to properly aggregate, analyze and report on these issues, across your enterprise, can provide a great deal of insight into enterprise security while removing one of the largest burdens to system administration. An Enterprise Event Correlation System should be able to receive log and audit data from all of the servers, applications and devices in your enterprise, and alert you to security-related incidents and deviations from your corporate security policies. An added benefit of a sound Event Correlation Engine is a self-checking mechanism to ensure that all of your security mechanisms are constantly working.

Other Security Tools

There are many other tools and technologies that are available and pertinent to business information security today. Encapsulated here is merely a general overview of the necessity and a review of issues related to the more common ones. Do not limit your technological search to the areas we have covered, but rather use them as a starting point in your analysis and evaluation of security methods, tools and systems appropriate to your specific needs.

Step 5: Implement and Educate

Once the necessary support has been garnered for the security plan, it is time to begin rollout. The technical details of any implementation will vary greatly depending on the environment, technologies, and skill sets of those involved, but there is one global part to security implementation that must never be overlooked: education. For any security initiative to be successful, the end users must receive education, which should include:

- Details and training on the operation of the new security systems/procedures
- An understanding of the effect of the new procedures on company data/assets
- Explanation of the procedures and how they fulfill the goals of the security policy

In short, do not just train your users on how to do something, but educate them as to why what they are doing is essential to the company as a whole. Once they believe the extra steps involved in providing information security can directly affect the company's bottom line, they will be much more likely to accept and adhere to them.

Step 6: Continually Examine, Analyze, and Act

The most important aspect of any security system is the diligent, continual monitoring of system and device events. Constant consolidation and analysis of all event messages from firewalls, IDS's, VPN devices, routers, servers, and applications is the only way to truly evaluate the continued effectiveness of a security implementation, and the only way to detect many of the most common breaches of security and policy violations.

This also applies to corporate security policies and procedures, as well as the involvement of the Security Steering Committee in the business process evaluation. Keeping the committee involved in new security issues and technologies, and constantly reassessing and updating the security policy will ensure that awareness of security stays at the forefront and will help ensure that issues and opportunities don't fall by the wayside.

Practical Recommendations for System and Network Security

Up to this point, we have concentrated mainly on the logical and systematic steps necessary to provide an enterprise security system. From here on, we will address some of the specific steps that can be taken to improve security, based on the results of External Perimeter Assessments and Internal Security Assessments conducted by Solutionary, Inc. We are limiting the scope of these recommendations to common issues we have encountered over the last six months, in order to provide a more accurate description of the issues and challenges facing corporate networks today. To better help the IT professional, these recommendations are divided into platform sections.

Windows NT/IIS

- Almost 95% of the NT/IIS issues we have seen can be resolved with one word: patch. Make sure all NT and IIS servers are patched to the latest levels and the level of vulnerability and risk will drop substantially.
- Delete (or don't install) all sample scripts from Internet web servers
- Don't install unnecessary applications on servers (Office, Outlook, etc.)
- Disable any services and devices that aren't required

Cisco Routers

- Disable finger, telnet, and other services/ports on the router.
- Don't run HTTP daemon.
- Drop IP source-route packets.
- Run Unicast RPF to prevent your users from spoofing packets.
- Use your router as a pre-firewall by implementing ACLs similar to your firewall rules.

General Firewall Configuration

- If you don't need it, don't allow it! Your firewall configuration should contain explicit rules for only the traffic you need to allow in, and block everything else.
- Minimize remote access to the firewall.
- Provide a revision control system for firewall rules.
- Test rules!

Cisco PIX Firewalls

- Don't allow telnet access
- Employ AAA for system/console access

Checkpoint Firewall-1

- Disable the default rules to allow encryption and management of the firewall, replacing these implied rules with specific rules for your implementation.
- Don't use the default 'allow DNS traffic' rule – accept DNS traffic only to those servers providing external DNS.

Internal DNS

- Any servers providing internal DNS and recursive services must not provide external DNS as well.
- Check with your DNS vendor to configure protection from cache poisoning.

What's next?

The suggestions found in this paper are not a one-time checklist to better security; rather they are a starting point to create a comprehensive, enterprise-wide outlook towards the protection of company assets and information. It is important to remember that at no time can you rest on your previous actions or decisions, because new security issues, vulnerabilities, and exploits are constantly being created. Security is nothing if not an evolutionary process: a vulnerability is discovered, an exploit is created and a patch is applied. This process occurs over and over again in today's technological world, and the timeframe between vulnerability discovery and exploitation continues to shorten.

With this in mind, the most important method of protecting your assets is the diligent monitoring of any and all security measures in place. Firewalls, IDS's, servers, and applications all provide volumes of information regarding attacks – both successful and unsuccessful. By constantly monitoring and analyzing this information, it becomes possible to understand the level of threat faced by your organization and respond in a timely manner to the true threats that occur.